Testimony of Guy L. Copeland
Chairman, Information Technology Sector Coordinating Council

Before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity, Committee on Homeland Security,
United States House of Representatives

Hearing on
"The Future of Cyber and Telecommunications Security at the Department of Homeland Security"

September 13, 2006

Mr. Chairman, distinguished members of the Subcommittee, thank you for inviting me to testify before you this afternoon. On behalf of the members of the Information Technology Sector Coordinating Council, I commend you for your continuing attention to Cyber and Telecommunications Security.

Five years ago this week, we suffered the most devastating, terrorist attack in the history of our nation. The deliberate, horribly evil assaults on that day did not include a cyber attack. But they immediately reaffirmed how dependent we are on our information technology and communications sectors to respond quickly and effectively in any emergency and to recover and reconstitute normal societal functions. Subsequent analysis also showed that the technologies of these two sectors are equally crucial to prevention and preparedness at all levels.

A little over a year ago now, Katrina painfully reminded us that natural emergencies can be devastating. The scale of Katrina's impact and the response required was unprecedented. Once again though, communications and information technology were essential to response, recovery and reconstitution. Lessons learned have since been folded into the preparedness posture and emergency plans of the critical institutions, both industry and government.

My testimony today is based, in part, on my experiences and observations on how we have reacted to these and other tragedies. I've formed these observations, in part, based on my experience as Chairman of the Information Technology Sector Coordinating Council (IT SCC) and the immediate past President of the Information Technology Information Sharing and Analysis Center (IT-ISAC). Additionally, I am drawing on my experience as Vice President of Information Infrastructure Advisory Programs at Computer Sciences Corporation (CSC). However, I must emphasize that I am not speaking on behalf of CSC, the IT SCC or the IT-ISAC. I am offering my personal reflections, previously shared with key leaders in each organization.

We – both the Private Sector and Government - have been building an increasingly strong partnership, starting long before DHS was created. The level and sophistication of activities and initiatives has grown tremendously during that period. As the Information Technology sector witness today, I am focusing my comments in that sector. But I am equally proud of the efforts of my friends, colleagues and others who are equally dedicated to our common cause in their

respective sectors. Many companies – large and small – are among our best citizens in terms of their selfless contributions.

IT SCC

In January 2005, while then serving as the President of the Information Technology Information Sharing and Analysis Center (IT-ISAC), I briefed a joint industry and government group on an initial proposal to begin an effort in the IT sector to consider the formation of the IT Sector Coordinating Council (IT SCC). Working with Mr. Harris Miller, President of ITAA, the leadership of the IT-ISAC and other sector leaders and with the facilitation assistance of Meridian Institute provided by DHS, we developed the necessary formation documents through 2005. In November 2005, we announced the interim IT SCC and in January 2006, the formal charter, first slate of officers and the executive committee were approved by over thirty founding members.

As with SCC's representing electricity, financial services, telecommunications, water, transportation, and others, the IT-SCC was organized to serve as a central point of coordination, collaboration and information sharing among the many members of the sector, and with the Federal agency(ies) responsible for interacting with a given private sector on critical infrastructure protection. The Department of Homeland Security – specifically the National Cyber Security Division (NCSD) - is the designated Sector Specific Agency responsible for collaborating with the IT sector.

In January, the IT-SCC completed its formation procedures, ratified its operating charter, and elected its leadership. With Harris's departure from ITAA, Greg Garcia, ITAA's Vice President for Information Security, was elected to the SCC's Executive Committee, as the Secretary. I was elected Chairman; Michael Aisenberg of VeriSign, Vice Chairman; and Larry Clinton of the Internet Security Alliance, Treasurer.

During and since its formation, the leadership and members of the IT SCC have been actively engaged in collaborative partnership with their government colleagues. We were invited to participate fully in the update of the National Infrastructure Protection Plan (NIPP) and our plans committee, under the leadership of Paul Kurtz of the Cyber Security Industry Alliance and John Lindquist of EWA, has formed a joint writing effort with our government colleagues, led by Cheri McGuire of the NCSD at DHS, to draft the IT Sector Specific Plan (SSP) which will in a few months be completed, staffed with our respective IT SCC and IT Government Coordinating Council membership, and approved as an annex to the NIPP. This joint effort exemplifies a marked improvement in the partnership as compared to the earliest days of DHS. The leadership on both sides should be commended for the strides that have been made.

IT sector leadership has been pleased with the relationships we have developed with the current leadership within DHS. In particular, Under Secretary for Preparedness, the Honorable George Foresman: Assistant Secretary for Infrastructure Protection, Mr. Robert Stephan, and Acting Director of the National Cyber Security Division, Mr. Donald "Andy" Purdy, have all worked tirelessly to include us in initiatives that affect the private sector. They have provided encouragement and support. They have been open to consideration of our recommendations. They have included us in the development of key documents such as the recent National Infrastructure Protection Plan (NIPP). Recognizing the importance of cyber securityand

communications, Undersecretary Foresman has recently directed his Deputy Under Secretary, Robert Zitz, to provide day-to-day oversight of the NCSD and the National Communications System, which together constitute the new Cyber Security and Telecommunications organization. Our leadership has met with Mr. Zitz and we are impressed with how quickly he has picked up the reins and the approaches he is espousing. In short, they are trying as hard as anyone can -- within current government restrictions on private sector relationships -- to develop, nurture and grow a valuable and essential partnership for critical infrastructure protection.

There are many challenges remaining for us to address and new ones are sure to arise. We look forward to meeting those challenges with them and with their successors.

IT-ISAC and the ISAC Council

PDD 63 called for industry establishment of Information Sharing and Analysis Centers (ISACs). The Information Technology (IT) sector coordinator, Mr. Harris Miller, President of the Information Technology Association of America (ITAA) and other sector leaders began developing the necessary charter documents and reaching out to potential members. On January 16, 2001, in a press conference held at the Department of Commerce, 19 founding members formally announced the IT-ISAC. The mission of the IT-ISAC is to provide

- Trusted and confidential reporting, exchange and analysis of sensitive cyber and physical information concerning incidents, threats, attacks, vulnerabilities, solutions, countermeasures, and best security practices.
- A trusted mechanism enabling the systematic and confidential exchange of member information with strong and enforceable legal protections.
- Leadership visibility for IT-ISAC members with public and private enterprises on cyber security processes and information sharing issues.

A sampling of the value of IT-ISAC membership includes:

- Access to Sensitive Threat, Vulnerability and Analytical Products
- Collaboration in a Trusted Forum - vetted, trusted and confidential
- Anonymity for Members - within industry and to government
- Access to Cross Sector and Government Information, Contacts and Tools
- Emergency Response Coordination, Operational Practices, and Exercises

In July 2001, the IT-ISAC went operational through a 24/7 operations center manned by their contract with Internet Security Systems. July 2001 also found them helping coordinate the response to a new form of malicious software, Code Red. On September 11, 2001, they helped to support the response activities and a few days later helped to coordinate the response to another cyber threat, NIMDA.

In 2002, the IT-ISAC established formal information sharing memoranda of understanding (MOUs) with the Financial Services, Electricity and Communications ISACs. In 2003, it helped to establish the ISAC Council, an informal, voluntary, cross-sector body, consisting of the leadership of the active sector ISACs. Mr. John Sabo, the current IT-ISAC President, is also the current Chairman of the ISAC Council. 2003 also saw the IT-ISAC start daily cross-sector cyber security collaboration calls for all ISACs and government agencies (including DHS) which adhere to the MOU information sharing agreements.

Since then the IT-ISAC has continued to mature and expand its capabilities. In 2005, they hired a full time Executive Director, Mr. Scott Algeier. In addition to the daily cyber calls, they host twice weekly cyber technical calls which can dive deeply into technical issues and analysis, for example, those associated with emerging exploits or newly released patches. And they have recently added a weekly physical issues call which supports cross-sector sharing of information regarding physical incidents, vulnerabilities and related matters.

Throughout 2005, IT-ISAC leadership was at the forefront of efforts to form an IT Sector Coordinating Council (IT SCC). SCC's were requested of the critical infrastructures by DHS and Homeland Security Presidential Directive 7 (HSPD 7) and further detailed in the National Partnership Model of the President's National Infrastructure Advisory Council (NIAC). SCCs are intended to be broadly representative of their sector and to work with DHS, Sector Specific Agencies (SSAs) and other organizations in developing strategies and policies for critical infrastructure protection. In January 2006, the IT SCC was formalized and in May it recognized the IT-ISAC as the sector's official operational information sharing mechanism.

> "For operations, analysis and information sharing, the Information Technology Information Sharing and Analysis Center (IT-ISAC) is recognized and endorsed by the Information Technology Sector Coordinating Council (IT SCC) as our lead for the IT sector. The IT-ISAC has served since 2001 and will continue to serve as the main vehicle for communicating information about threats, vulnerabilities and incidents, especially through its Operations Center on a 24/7/365 basis. It is also our main vehicle for information analysis."
>
> IT SCC Chair and Vice Chair Letter to Asst. Sec. Robert Stephan dated 5/26/06

Looking to the Future

Assistant Secretary for Cyber Security and Telecommunciations

In his Second Stage Review, Secretary Michael Chertoff proposed the establishment of an Assistant Secretary position for cyber security and telecommunications to "centralize the coordination of the efforts to protect the technological infrastructure."[1]

The IT Sector Coordinating Council, the IT-ISAC, and the other bodies I have briefly described, stand ready to welcome and work with the new Assistant Secretary from the moment he or she is announced. We have no doubts that it is in the interests of all of us to partner with him or her to address our common security concerns which cannot be addressed by each of us alone.

Even before announcement by DHS of this Assistant Secretary position, the IT Sector leadership had long advocated a senior Cyber Security executive (IT and Communications) for long term leadership, visibility, making the case for resources, and giving the issue area stature commensurate with the growing risks as IT and Communications become ever more critical to so many of our most important societal functions. The ideal appointee to this new position

- must be credible to both government and industry,
- must be open to new ideas and recognize the value of experienced input,
- must be a strong leader who can build and maintain trusted partnerships, and

[1] "Statement of Secretary Michael Chertoff, U.S. Department of Homeland Security, Before the United States Senate Committee on Commerce, Science, and Transportation." July 19, 2005.

- must convey and get support for a vision of success and a path to achieve it.

In addition, he or she will need the commitment of DHS and Administration leadership to succeed. That commitment must strive to ensure the new Assistant Secretary is

- empowered and supported with the resources to succeed,
- supported by positive, "can-do" legal advisers willing to break new ground for the close, trusted relationships required for critical infrastructure protection,
- unhampered to readily and effectively partner and communicate with the private sector, including
    - unhampered by administrative and bureaucratic trivia,
    - unhampered by excessive diversion from priorities, and
    - unhampered by well meaning but inappropriately applied restrictions.

Prioritize and Focus

The new Assistant Secretary must avoid and be protected from chasing the issue of the day or week. To avoid that trap, he or she must ensure that lower priorities are handled as and where needed in the organization but focus his or her attention and that of senior management and oversight on the main priorities

Congress can help empower the new Assistant Secretary by helping to set the right priorities, ensuring resources to achieve them, removing inappropriate and hampering restrictions and providing oversight to the priorities while avoiding diversion of time and attention to minor items

Trusted Partnership

Trusted partnership is a key, critical priority. For critical infrastructure protection, the directly involved key personnel from Government and industry must develop into a well trained, close knit team. The current leadership at DHS has made huge strides to improving partnership but still appear to be hampered by perhaps conservative interpretation and application of laws and regulations rightly intended for protection of a procurement or regulatory relationship, not the national security partnership that Homeland Security needs. Our sectors are complex, evolutionary and robust. Regulation and mandates cannot achieve the intelligent preparedness and response capabilities that thoughtful, voluntary partnership and teamwork can achieve. The best partnership and teamwork is fostered through physical co-location and daily interaction in planning, training and executing – just as in any successful sports team or military unit.

Physical Co-Location for Crisis Coordination - Build on the NCC

A top priority for continuing preparedness and timely response must be physical co-location and frequent daily interaction of representatives of all key players – industry and government - for crisis response management. Ultimately, we execute well that which we develop thoughtfully and practice carefully, learning and improving as we go. Writing a plan for winning isn't enough. I suggest that DHS build on the 20+ years experience with the NCC. Continue to strengthen NCC interoperation with other key 24/7 operations such as those operated by ISACs. Add representatives from other, time-critical ("millisecond sectors"). Add others in time, with core group representation (i.e., representation from the most important organizations for response in the sector or entity.)

National Crisis Coordination Center

The concept of a jointly (industry and government) manned, National Crisis Coordination Center has been around for at least a few years now. In 2004, the Early Warning Task Force begun as one of the National Cyber Security Summit task forces, recommended[2] creation of a national crisis Coordination Center to:

· House government, industry and academic security experts, both physical and cyber, to bridge the cultural barriers that have hampered a true partnership in counterterrorism and cyber security

· Jointly prepare, exercise, evaluate and update National Joint Crisis Response plans to prevent, detect and respond

· Operate joint watch centers

· Conduct joint exercises at the national level to train and test the plans

· Conduct joint field training at the regional level to train and further test the plans

· Respond jointly to traditional natural events, as well as malicious events

· Proactively share intelligence – both national security and law enforcement

· Include a secure, compartmented intelligence facility staffed equally with government and private sector representatives, as well as appropriate state, local and other representation

· Proactively address priority remediation of systemic vulnerabilities in national level infrastructures

In March 2006, the NSTAC's Next Generation Networks Report recommended a Joint Coordination Center.[3]

> "A joint coordination center for industry and Government should be established. This would be a cross-sector industry/Government facility with a round-the-clock watch, and would be brought up to full strength during emergencies. Such a center would improve communications between industry and Government as well as among industry members, and would incorporate and be modeled on the NCC.
>
> "The center should be a Government-funded, appropriately equipped facility, manned jointly by experts from all key sectors. In a fully converged NGN environment, everything will be interconnected and interdependent to a greater degree, and thus means of coordinating among all key sectors must exist. Physically collocated, joint manning is vital to achieve the high level of interpersonal trust needed for sharing sensitive specific information and to achieve the level of mutual credibility required in a fast-paced decision-oriented environment. It should provide the full set of planning, collaboration, and decision-making tools for those experts to work, whether together as a whole or in focused subgroups. Industry is at times hesitant to share information with the Government because it is unsure of how the information will be used, and Government-to-industry information sharing should also be improved.[4] DHS has a vision for how HSOC will function to improve information sharing; however, the HSOC's current operational interface to the private sector [the National Infrastructure Coordination

---

[2] National Early Warning Task Force Recommendation, A NATIONAL CRISIS COORDINATION CENTER, National Cyber Security Partnership, March 2004

3 Next Generation Networks Task Force Report, NSTAC, March 28, 2006.

4 Both these observations were confirmed at the August 2005 NGN Incident Response Subject Matter Experts meetings. See Appendix D of the Next Generation Networks Task Force Report, NSTAC, March 28, 2006.

> Center (NICC)] is nascent and needs further development. An environment of trust must be established. A joint operations center could play a key role in fostering that environment and in enhancing HSOC operations. In addition, appropriately cleared industry experts collocated in a joint coordination center with their Government counterparts could assist the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), the DHS intelligence analysis arm, in performing its analytical and reporting functions, helping to ensure that HITRAC products are more complete, credible and useful."

The Inspector General at DHS has also stated, "If the partnership between the federal government and private sector is to be successful, another key requirement is establishing a permanent physical location or forum so that critical and non-critical sectors can interface with one another and their federal counterparts. This is essential to developing and maintaining long-term collaborative relationships."[5]

NCC Relocation – an Immediate Concern

Since its establishment, the National Coordinating Center for Telecommunications (NCC) has been housed in the Defense Information Systems Agency (DISA) headquarters facility. That location was natural because the same facility housed the National Communication System (NCS) which served as the support Secretariat for the NSTAC and also was assigned responsibility for the jointly manned NCC. That location turned out to be invaluable for trusted, sensitive information sharing. It also housed or came to house DISA's Global Network Operations and Security Center (GNOSC) and its subordinate Defense Department computer emergency response team (CERT), and the Department of Defense Joint Task Force - Global Network Operations (JTF-GNO). The synergy and trusted interaction between and among these entities has become important to all participants for both national security and emergency response purposes. Unfortunately, current plans call for relocating the NCC to co-locate it with the US-CERT operated by DHS.

We should strongly consider the wisdom of separating the NCC from the DoD entities with which it is located. Instead we should encourage the leadership of the DoD, DISA and DHS to consider an approach that could strengthen the value for all: co-locate the US-CERT and other NCSD operational response elements with the NCC and their counterpart DoD elements. While each has a different mission and set of customers, they are all ultimately looking at overlapping sets of data and similar problem sets. Co-location will allow for greater interaction and synergy, leading to enhanced efficiency and value for all their "customers."

Because the Base Realignment and Closure process is expected to relocate DISA in a few years, part of the examination of the value for the nation in achieving multi-organization co-location will have to be an examination of facility alternatives. But that should not deter us from at least exploring the potential benefits that could be achieved for the nation and both our national and homeland security. Ultimately, the co-location facility could be part of the National Crisis Coordination Center which I have already described.

My industry colleagues and I would be happy to participate in such an examination.

Congress Can Help

[5] A Review of the Top Officials 3 Exercise, DHS OIG Report OIG-06-07, p. 24 (Nov. 2005).

Support Examination of NCC Co-location and Expansion to a National Crisis Coordination Center

Look at co-location of the NCC, the US-CERT, the JTF-GNO and other existing similar entities for advantages to their missions, their "customers" and the nation. Similarly, examine the National Crisis Coordination Center (NCCC) concept in detail and strongly support its implementation if it holds up to your scrutiny as many of us expect it will. Be sure to include international liaison in the NCCC. Many of our allies are even more closely intertwined with us in the Cyber world than in the physical world. But in both, the interdependencies can be enormous. In particular, with Canada, many of our key critical infrastructures and dependencies are mutually shared across our common border.

Focus on Priorities

Use your oversight and appropriations powers to work with DHS and the private sector in the establishment of Cyber Security priorities. Then follow-up to ensure DHS has the necessary resources to implement those priorities.

Create a Better Environment

Congress can create a better environment for homeland security partnership, helping us achieve a tight knit, superbly prepared, professional team with high morale, and a commitment to each other to succeed. The current environment for government and industry interaction is designed rightly to prevent fraud and abuse in procurement or regulatory matters or other areas where an unscrupulous actor might try to further a personal or organizational agenda, contrary to the public good. In many ways, those rules implicitly require Government personnel to maintain an "arms length," almost adversary relationship. At the very least, it implicitly impugns motives before the fact. But Homeland Security partnerships must be close, trusted, and non-public. Could the Washington Redskins or any professional team succeed if their members were not allowed to get together to plan and train out of sight of their opponents when needed?

We cannot do away with protection against fraud and abuse. But the close teamwork and rapid response requirements of Homeland Security and Critical Infrastructure Protection demand high levels of interpersonal trust that can only be developed through frequent interaction, including informal, relationship building interaction. To accomplish this and still protect against fraud and abuse, I believe that we will need to replace the rigid rules and bureaucratically slow exception handling processes with alternative systems that provide strong, independent oversight to detect, report, halt and punish fraud and abuse but encourage true partnership, trusted relationships and team building, treating all participants as if they are members of the same organization/team, operating under the same code of ethics but free to form trusted and close relationships.

Examine Innovative Ways to Encourage Private Sector Active Participation

Congress might be able to help encourage even more private sector participation in critical infrastructure protection through private sector bodies such as the SCCs and ISACs. Here are a few examples which might be worth exploring.

Value Proposition

Congress and the DHS should work with SCCs, ISACs and other private sector institutions to develop a compelling value proposition with industry to further improve our working relationship for critical infrastructure protection and expand improved cyber security behavior. Not doing so is contrary to our national and homeland security interest. Many companies and other private sector institutions understand this. But many still do not. We need to make the value proposition compelling so that the vast majority – and all the critical ones – understand and pro-actively participate.

Congressional and Executive Support for SCCs and ISACs

Carefully examine the positive role that DHS and Administration executive leadership could and should play in encouraging sector members to participate in their respective SCCs and ISACs. Private sector leaders responded to previous Government requests and have expended significant resources to create the partnership model organizations requested. But when it comes to encouraging sector members to join those bodies and actively participate in them, Government executives have been strangely absent or quiet for the most part. Also, in some cases they have reached out through other organizations not formed for these specific purposes. The net effect of their silence or misaimed outreach is contrary to the very goals they envisioned achieving when they asked the private sector to form ISACs and SCCs.

Simply put, they should always turn first to the organizations they asked us to form to fit their model for working with them. And they should not be shy about encouraging sector members to join those organizations (ISACs and SCCs), even to the extent of expressing unhappiness with important sector "core" players who fail to do so. If there are any rules in place that impede such demonstrable support, they should be revisited swiftly and decisively.

Technical and Operational Support

The ultimate goal of our partnership model is to create an infrastructure environment that is intended to deter attacks as much as feasible and operationally prepared to respond, recover and reconstitute to any attack or emergency as rapidly and effectively as feasible. Operational preparedness and success will depend ultimately on a partnership that is focused on operations even more than on policy. The recommendations I have made for a jointly manned, National Crisis Coordination Center (NCCC) will help significantly to shift to an operational focus. But it will also take working out and testing our individual and collective Concepts of Operations (CONOPS), constantly improving them so our operational metrics continually improve. The best solutions may call for cross sector or even government to industry provisioning of technical and operational support. For example, DHS support to operational ISACs might be appropriate. Operational readiness and improvement should be one of our highest priorities.

Congressional Charters

Examine the Potential Value of a Congressional Charter for established SCCs and ISACs. If a National Crisis Coordination Center is supported, consider a Congressional Charter for it as well. Congressional Charters would give Congress enhanced visibility into their

functioning and would allow for periodic GAO audit. They would also help many SCCs and ISACs recruit the broad membership and participation they need from their sectors.

Procurement

Consider using procurement in DHS, or even government-wide, as a carrot for greater private sector participation and proactive, operational commitments.

Congressional Awareness and Education

Finally, to help prepare you for the increasingly complex issues of the Cyber Security Age, I suggest you consider forming a bipartisan House caucus for cyber security (IT and communications) to provide a forum for educating staff and members on the relevant issues

Summary of a few Key Cyber Security and Telecommunications Partnerships and Key Initiatives

Attachment To

Testimony of Guy L. Copeland
Chairman, Information Technology Sector Coordinating Council

Before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity, Committee on Homeland Security,
United States House of Representatives

Hearing on
"The Future of Cyber and Telecommunications Security at the Department of Homeland Security"

September 13, 2006

NSTAC

President Ronald Reagan created the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382 in September 1982. Composed of up to 30 industry chief executives representing many of the major communications and network service providers and information technology, finance, and aerospace companies, the NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy. Since its inception, the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns.

NS/EP communications enable the Government to make an immediate and coordinated response to all emergencies, whether caused by a natural disaster, such as a hurricane, an act of domestic terrorism, such as the Oklahoma City bombing and the September 11th attacks, a man-made disaster, or a cyber attack. NS/EP communications allow the President and other senior Administration officials to be continually accessible, even under stressed conditions.

The NSTAC has addressed numerous issues in the past 24 years. A few examples illustrate NSTAC's capabilities to address NS/EP communications issues in today's environment: the establishment of the National Coordinating Center for Telecommunications (NCC); the implementation of the Government and NSTAC Network Security Information Exchange (NSIE) process; the Telecommunications Service Priority (TSP) program; Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS); and the examination of the NS/EP implications of Internet technologies and the vulnerabilities of converged networks. These accomplishments are briefly described below.

NCC – From "NSTAC Report to the President on the National Coordinating Center," May 10, 2006

The NCC was established to fulfill a critical need for a national coordinating mechanism to organize and manage the initiation and restoration of NS/EP communications services. This need was identified at the dawn of the divestiture of AT&T and the height of the Cold War. As Government increasingly relied on commercial communications services and no longer had a single point of contact (POC) for the industry, Government needed a joint industry and Government-staffed organization to coordinate emergency requests. The NCC became operational on January 3, 1984.

The National Coordinating Center (NCC) has been the hub for coordinating the initiation and restoration of national security and emergency preparedness (NS/EP) communications services for more than 20 years—supporting four administrations and evolving as threats and national priorities have shifted. Following the September 11, 2001, terrorist attacks, the NCC proved its value to the Nation as it supported the restoration of communications in the New York and Washington, D.C., areas. The NCC has also repeatedly shown its strength during hurricane recovery efforts, including Hurricane Katrina.

... the NSTAC recommended designating the NCC as the Information Sharing and Analysis Center (ISAC) for telecommunications in 1999.

With the establishment of the Department of the Homeland Security (DHS) and the transfer of the National Communications System (NCS) to the new department in 2003, the NCC also has made the transition to DHS.

The primary mission of the NCC throughout its history has been to coordinate the restoration and provisioning of communications services for NS/EP users during natural disasters, armed conflicts, and terrorist attacks. Significant events such as the Hinsdale, Illinois, central office fire, the Oklahoma terrorist bombing, the events of September 11, 2001, and Hurricane Katrina have proved the value of this partnership. During a crisis, Government personnel communicate NS/EP requirement priorities to industry, and industry representatives assist the Government in developing situational awareness by providing restoration status information. Having the representatives in one location ensures a smoother restoration effort. The NCC's all-hazards response depends on the flexible application of NCS resources, such as its priority service programs (e.g., Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority [TSP] Program).

During day-to-day operations, NCC members work on plans and share information on vulnerabilities and threats to the telecom infrastructure. Planning activities include developing lessons learned following events, creating comprehensive service restoration plans, planning for continuity of operations (COOP)/continuity of Government (COG) activities, and participating in exercise planning. In addition, the NCC works with international emergency response partners, including the North Atlantic Treaty

Organization (NATO), International Telecommunication Union (ITU), and Canada, on crisis communications and mutual assistance.

In 2000, the NCC was designated the ISAC for telecommunications per the guidance in the 1998 Presidential Decision Directive 63 (PDD-63), Protecting America's Critical Infrastructures, which encouraged the private sector to establish ISACs to "serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information." As part of the ISAC mission, the NCC collects and shares information about threats, vulnerabilities, intrusions, and anomalies from the communications industry, Government, and other sources. Analysis on information is performed with the goal of averting or mitigating impact on the communications infrastructure.

The NCC has historically been an operational element and as such does not fall under provisions of the Federal Advisory Committee Act (FACA). A June 1, 1983, letter to the NCS from Assistant Attorney General William F. Baxter discussed issues of incident management and information sharing for the proposed National Coordinating Mechanism (NCM) (which became the NCC) and noted that such an organization posed no significant antitrust problems.

… Since the transition to DHS, the NCC has been involved in additional critical infrastructure protection (CIP) activities. As part of the implementation of Homeland Security Presidential Directive (HSPD) 7, DHS is tasked with identifying, prioritizing, and protecting the Nation's critical infrastructure. Through the NCC, the NCS often coordinates data calls on the identification of assets, coordinates planning for national special security events (NSSE), and provides impact analyses. In the future, NCC industry members may be asked to further assist in the risk assessment process as detailed in the sector's Sector-Specific Plan.

NSIE – From "GUIDE TO UNDERSTANDING THE NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS AND THE NETWORK SECURITY INFORMATION EXCHANGES," PREPARED BY THE OFFICE OF THE MANAGER, NATIONAL COMMUNICATIONS SYSTEM, MARCH 2001

In April 1990, the Chairman of the National Security Council's (NSC) Policy Coordinating Committee- National Security Telecommunications and Information Systems requested the Manager, NCS, identify what action should be taken by Government and industry to protect critical national security telecommunications from the "hacker" threat. … In response to the NSC tasking, the Manager, NCS and the NSTAC established separate, but closely coordinated, NSIEs. In May 1991, the NSIE charters were finalized, and Government departments and agencies and NSTAC companies designated their NSIE representatives, chairmen, and vice-chairmen. The first joint meeting of the Government and NSTAC NSIEs was held in June 1991.

The Government and NSTAC NSIEs meet jointly approximately every two months. The NSIEs provide a working forum to identify issues involving penetration or manipulation

of software and databases affecting NS/EP telecommunications. The NSIEs share information with the objectives of:

· Learning more about intrusions into and vulnerabilities affecting the PN · Developing recommendations for reducing network security vulnerabilities
· Assessing network risks affecting network assurance
· Acquiring threat and threat mitigation information
· Providing expertise to the NSTAC on which to base network security recommendations to the President.

The success of the NSIEs is based in large part on the establishment of trusted interpersonal relationships. Participants – government and industry – must hold requisite security clearances and sign individual non-disclosure agreements. The organizations sending participants to the NSIEs must also sign organizational non-disclosure agreements.

TSP – From NCS Web site

Telecommunications Service Priority (TSP) provides service vendors with a Federal Communications Commission (FCC) mandate for prioritizing service requests by identifying those services critical to NS/EP. A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service.

From briefing "NCS Roles During the Attack on America," Deputy Manager, NCS, August 9, 2002

- *Nearly 40,000 TSP circuits enrolled by NCS prior to 9/11 tragedy*
  - *TSP vital in accelerating the opening of Wall Street on 9/17*
    - *Major coordination in restoration of telecommunications for Broad Street switches – major role to restore stock and bond markets*
  - *NCS supported nearly 600 provisioning requests following 11 Sep 01*
    - *46 organizations (incl. FBI, FEMA , FRB, Port Authority, DoD)*

GETS – From NCS Web site

Implemented in the early 1990's, Government Emergency Telecommunications Service (GETS) is an emergency phone service provided by the National Communications System (NCS) in the Information Analysis and Infrastructure Protection Division of the Department of Homeland Security. GETS supports federal, state, local, tribal, industry, and non-governmental organization (NGO) personnel in performing their National Security and Emergency Preparedness (NS/EP) missions. GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN). It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.

From briefing "NCS Roles During the Attack on America," Deputy Manager, NCS, August 9, 2002

- *The AT&T long distance network carried a record 431 million call attempts on Sept. 11, 101 million more than the previous high-traffic day.*
- *Massive congestion in WTC & Pentagon areas*
  - *Over 10,000 GETS calls in WTC/Pentagon areas*
    - *Over 95% completion rate - Highest calling in first 48 hours*
  - *GETS PIN Cards:*
    - *Over 1,500 key personnel made GETS calls*
    - *Over 20,000 GETS PIN cards issued following events of September 11th*

WPS – From NCS Web site

Wireless Priority Service (WPS), is the wireless complement to GETS. In the early 1990's, the OMNCS initiated efforts based on NSTAC recommendations, to develop and implement a nationwide cellular priority access capability in support of national security and emergency preparedness (NS/EP) telecommunications and pursued a number of activities to improve cellular call completion during times of network congestion. Subsequently, as a result of a petition filed by the NCS in October 1995, the FCC released a Second Report and Order [FCC-00-242, July 13, 2000] (R&O) on wireless Priority Access Service (PAS). The R&O offers Federal liability relief for NS/EP wireless carriers if the service is implemented in accordance with uniform operating procedures. The FCC made PAS voluntary, found it to be in the public interest, and defined five priority levels for NS/EP wireless calls.

Wireless network congestion was widespread on September 11, 2001. With wireless traffic demand estimated at up to 10 times normal in the affected areas and double nationwide, the need for wireless priority service became a critical and urgent National requirement. In response, the National Security Council requested that the NCS deploy a nationwide priority access queuing system for wireless networks.

From briefing "NCS Roles During the Attack on America," Deputy Manager, NCS, August 9, 2002:

- *Verizon Wireless experienced a 50 to 100 percent increase nationwide. Wireless networks remained near saturation in NY through September 28th.*
- *Cingular Wireless' attempted calls ballooned by 400 percent in Washington and 1000 percent in its N.J. Switching Center*

PDD 63 and Sector Coordinators

Presidential Decision Directive 63 (PDD 63) was released in May 1998. It ordered the development of sector-specific critical infrastructure protection plans and established the role of private industry sector coordinators. The Information & Communications Sector as then designated under PDD 63, had four organizations sharing the sector coordinator role: the Cellular Telecommunications and Internet Association (CTIA), the Information Technology Association of America (ITAA); the Telecommunications Industry Association (TIA); and the United States Telecom Association (USTA).

Important early contributions of the Sector coordinators included

- developing internal sector awareness

- organizing voluntary sector participation in planning
- leading the way in the formation of Information Sharing and Analysis Centers for Information Technology and Telecommunications
- developing the I&C Sector National Strategy Input for Critical Infrastructure and Cyberspace Security, May 2002

PCIS

The Partnership for Critical Infrastructure Security (PCIS) consists generally of the leadership (usually the Chairs) of the organized Sector Coordinating Councils for the various critical infrastructures. The PCIS coordinates cross sector critical infrastructure protection interests and initiatives within the private sector and with the Government under the partnership model described within the National Infrastructure Protection Plan

NCSP (Santa Clara Dec 03 Summit, TFs, reports, Wye I, Wye II)

The National Cyber Security Partnership (NCSP) combines representatives from government, industry and academia working together to harden the nation's cyber defenses. The partnership provides a forum, structure and common agenda for interdisciplinary, cross-industry information exchange with government. Lead organizations of the partnership are: the Business Software Alliance, Information Technology Association of America, TechNet and the U.S. Chamber of Commerce. The public-private partnership was formed during the National Cyber Security Summit on December 3, 2003, in Santa Clara, California, which aimed to gather cyber security experts across disciplines to embark on a work program to develop recommendations for implementing key challenges posed in the 2003 National Strategy to Secure Cyberspace. The partnership established five task forces comprised of cyber security experts from industry, academia and government. Each task force was led by two or more co-chairs. The NCSP-sponsoring trade associations act as secretariats in managing task force work flow and logistics. The task forces included:

Awareness for Home Users and Small Businesses
Cyber Security Early Warning
Corporate Governance
Security Across the Software Development Life Cycle
Technical Standards and Common Criteria

The resulting task force recommendations in 2004 were provided to DHS. Many are still valid an valuable.

In follow-up to the National Cyber Security Summit and the reports of the task forces, DHS' National Cyber Security Division hosted a government and private sector exchange at the Wye River Conference Center in Maryland in January 2005. A second follow-up exchange ("Wye II") was hosted by the NCSP in Annapolis, MD, in September 2005. Many of the original Summit Task Forces' Recommendations continue to be brought up as potentially valuable.

CIPAC – extracted from DHS sources

In March 2006, the Department of Homeland Security established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate effective coordination between

Federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments.

The CIPAC represents a partnership between government and critical infrastructure/key resource (CI/KR) owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection.

CIPAC membership will encompass CI/KR owner/operator institutions and their designated trade or equivalent organizations that are identified as members of existing Sector Coordinating Councils (SCCs). It is also includes representatives from Federal, state, local and tribal governmental entities identified as members of existing Government Coordinating Councils (GCCs) for each sector

IDWG – extracted from DHS sources

The Internet Disruption Working Group (IDWG) is a DHS hosted, informal gathering of industry and government Internet technical operation experts who collaboratively explore vulnerability issues and identify recommended actions to address them. The IDWG is beginning to establish important, trusted interpersonal relationships amongst government and industry technical experts. The IDWG was established by NCSD in partnership with the National Communications System (NCS), in response to security concerns surrounding the growing dependency of critical infrastructures and national security and emergency preparedness users on the Internet for communications, operational functions, and essential services.

The IDWG's near-term objectives are to improve the resiliency and recovery of Internet functions in the event of a cyber-related incident of national significance; work with both government and private sector stakeholders to identify and prioritize protective measures necessary to prevent and respond to major Internet disruptions; and assess the operational dependencies of critical infrastructure sectors on the Internet. The 2005 IDWG Forum identified specific areas for action by both government and private sector stakeholders, including risk assessments, information sharing, protective measures, research and development, and Internet development issues. The IDWG is engaging with both public and private stakeholders to address these action items. The IDWG also plans to hold future forums and tabletop exercises, including an IDWG Tabletop Exercise, on June 15, 2006, to maintain both a pulse of the issues and an understanding of existing capabilities.